Performance Assurance Methodology & Techniques

October 2025~~4~~

Version 4.1~~0~~

RETAIL ENERGY CODE

Contents

1. Overview 7

2. Identifying Retail Risks 9

2.1 Defining Retail Risk 9

2.2 Sources of Retail Risks 10

3. Analysing Retail Risks 11

4. Assessing Retail Risks 12

4.1 Why do Retail Risks need to be assessed? 12

4.2 Analysis at Risk Driver level 12

4.3 Responding to Risk Driver scores 13

4.4 De minimis scoring 13

4.5 Data Cleanse 13

5. Performance Assurance Techniques (PATs) 16

5.1 Background 16

5.2 Methodology for Risk Management Determinations 17

5.3 Using data to make Risk Management Determinations 17

5.4 Governance of PATs 21

5.5 Communicating with Parties and Applying Techniques when a Potential Problem is Identified 22

5.6 Applying techniques when Escalation is Required 23

5.7 Applying techniques to Code Manager bodies and Service Providers 25

6. Preventive techniques 27

6.1 Provision of High-Quality guidance 27

6.2 Qualification / Maintenance of Qualification 28

6.3 Training and guided pathways 30

7. Incentive Techniques 32

7.1 Notification 32

7.2 Peer Comparison 33
7.3 Performance Charges 34
8. Risk Monitoring Techniques 37
8.1 Cross Industry Monitoring 37
8.2 Specific Topic Monitoring 39
8.3 Sentiment analysis 40
8.4 Surveys 41
9. Assessment Techniques 43
9.1 Enquiry 43
9.2 Information request (IR) 44
9.3 Self-assessment 45
9.4 Code Manager assessment 46
10. Remediation Techniques 48
10.1 Action plan 48
10.3 Management assertion 50
10.4 Code Manager / Independent validation 51
11. Escalation Techniques 53
11.1 Specific conditions 53
11.2 Referral to Ofgem 54
11.3 Event of Default 55
~~1. Overview ..... 5~~
~~2. Identifying Retail Risks ..... 7~~
~~2.1 Defining Retail Risk ..... 7~~
~~2.2 Sources of Retail Risks ..... 8~~
~~3. Analysing Retail Risks ..... 9~~
~~4. Assessing Retail Risks ..... 10~~
~~4.1 Why do Retail Risks need to be assessed? ..... 10~~
~~4.2 Analysis at Risk Driver level ..... 10~~
~~4.3 Responding to Risk Driver scores ..... 11~~

4.4 De minimis scoring 11
4.5 Data Cleanse 11
5. Performance Assurance Techniques (PATs) 13
5.1 Background 13
5.2 Methodology for Risk Management Determinations 14
5.3 Using data to make Risk Management Determinations 14
5.4 Governance of PATs 18
5.5 Communicating with Parties and Applying Techniques when a Potential Problem is Identified 19
5.6 Applying techniques when Escalation is Required 20
5.7 Applying techniques to Code Manager bodies and Service Providers 22
6. Preventive techniques 24
6.1 Provision of High-Quality guidance 24
6.2 Qualification / Maintenance of Qualification 25
6.3 Training and guided pathways 27
7. Incentive Techniques 29
7.1 Notification 29
7.2 Peer Comparison 30
7.3 Performance Charges 31
8. Risk Monitoring Techniques 34
8.1 Cross Industry Monitoring 34
8.2 Specific Topic Monitoring 35
8.3 Sentiment analysis 36
8.4 Surveys 37
9. Assessment Techniques 39
9.1 Enquiry 39
9.2 Information request (IR) 40
9.3 Self-assessment 41
9.4 Code Manager assessment 42
10. Remediation Techniques 44

10.1 Action plan 44
10.3 Management assertion 46
10.4 Code Manager / Independent validation 47
11. Escalation Techniques 49
11.1 Specific conditions 49
11.2 Referral to Ofgem 50
11.3 Event of Default 51

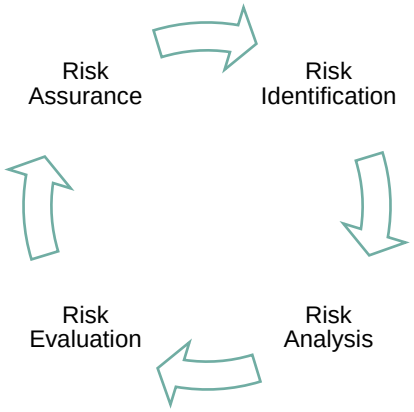
CHANGE HISTORY

Version	Status	Issue Date	Author	Comments
v1.0	Final	19/07/2021	The Code Manager	N/A
v2.0	Final	28/04/2023	The Code Manager	Annual Review
V3.0	Final	24/10/2023	The Code Manager	Updates to merge Performance Assurance Methodology and Performance Assurance Techniques into a single document. The Code Manager has also reviewed these documents in line with the Performance Assurance Operating Plan.
V3.1	~~Draft~~Final	23/04/2024	The Code Manager	Scheduled annual review
V4	Final	29/10/2024	The Code Manager	Scheduled annual review. Approved by PAB on 29/10/2024.
V4.1	Final	21/10/2025	The Code Manager	Scheduled annual review; minor housekeeping changes and added clarity on Data Cleanse

Performance Assurance Methodology

1. OVERVIEW

The REC Performance Assurance approach is risk based, with assurance activities driven by the risks to consumers and the effectiveness of the retail energy market. High or increasing risk will result in the application of one or more Performance Assurance Techniques (PATs).

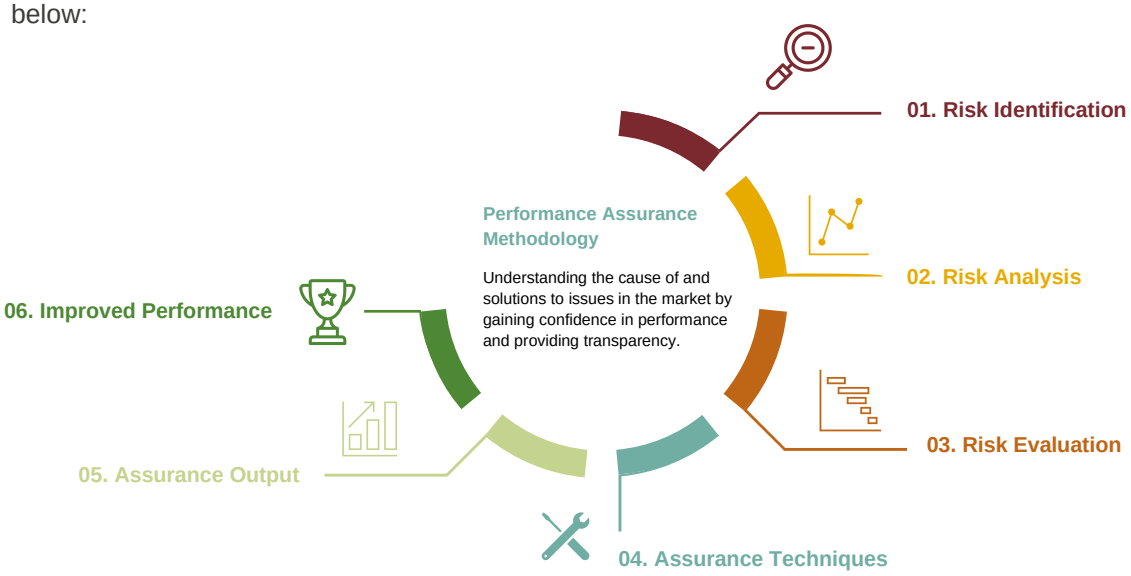


These techniques include creating incentives to improve performance, undertaking more risk monitoring and alerting, taking steps to prevent the risk resulting in an issue and assessing the risk in more detail.

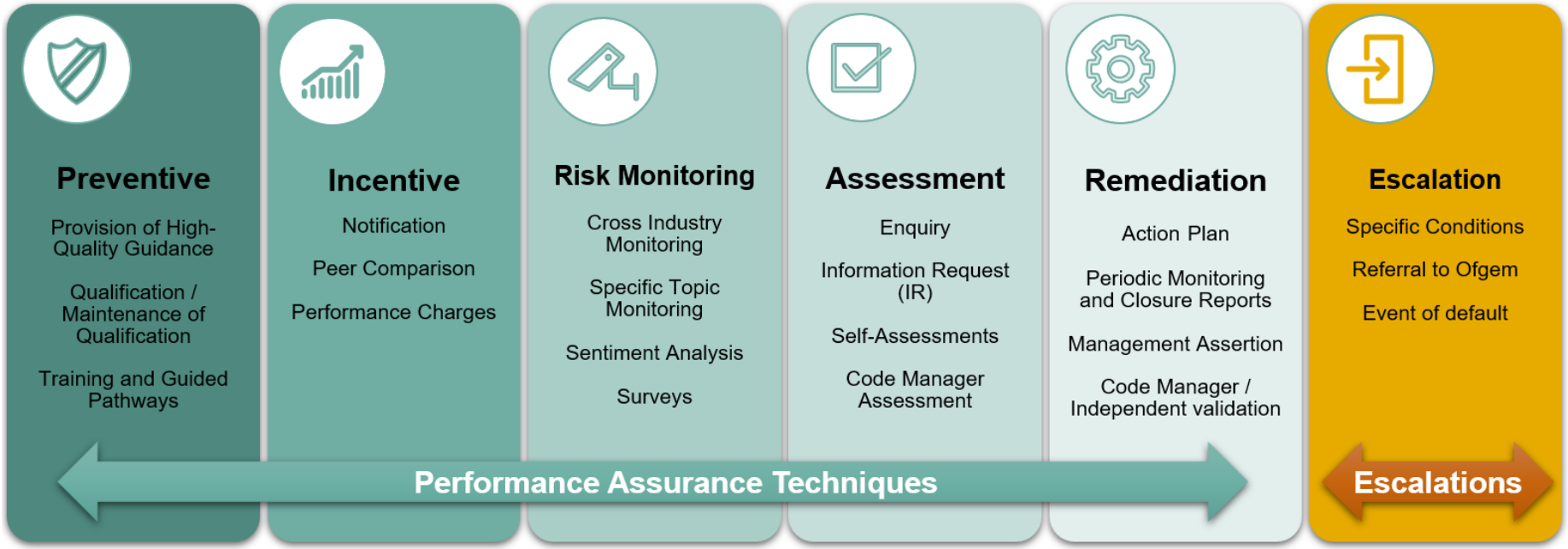
A core principle of the Performance Assurance Framework (PAF) is that it focuses on the root causes of risks and issues, so assessment activities may be industry wide where risk information suggests problems may be pervasive or focused on the performance of a particular party or group of parties.

This document covers the Code Manager's methodology for identifying, analysing, and evaluating risk, as well as how these processes interact with risk assurance. It also details the Performance Assurance Techniques (PATs) available to the Code Manager for risk mitigation and the methodology for applying them are set out in other elements of the performance assurance framework.

At a high level the risk assessment methodology, and the key inputs to it, are set out in the diagram below:



This document outlines the Performance Assurance Techniques (PATs) and further escalation techniques that will be used to drive high performance within the REC. Further detail on each one is included in sections 6 – 11.



2. IDENTIFYING RETAIL RISKS

2.1 DEFINING RETAIL RISK

The goals of the REC are established in the REC Objectives and mission statement, as set out below:



REC Objectives

a) to ensure the REC operates and evolves in a manner that facilitates the achievement of its mission statement;

b) to ensure customers interests and data is protected in the operation of the REC; and

c) to drive continuous improvements and efficiencies in the operation of the REC and the central systems and communication infrastructures it governs.

REC Mission Statement

Ffacilitate the efficient and effective running of the retail energy market, including its systems and processes...through promoting innovation, competition, and delivering positive customer outcomes.

The REC focuses on Retail Risks within the retail energy market. The Performance Assurance Schedule defines Retail Risk as:

> *'A risk that retail energy consumer outcomes or the effectiveness of the retail market are measurably and significantly degraded by a failure by a REC Service User or REC Service Provider to meet the objectives, standards or core processes under the REC.'*

To support the evolution of the Code we have taken the following steps:

- Structured our risk register around the REC objectives. Current risk drivers are mapped to processes, with SLA performance mapped to system performance.
- Mapped on improvement activities RECCo and the Code Manager are conducting to promote innovation, competition, positive customer outcomes and continuous improvement, as well as any assurance activities.
- Captured the inherent risk of any REC Party not meeting its REC obligations.
- Establishing a voice of the consumer to systematically measure if customer outcomes are positive and identify if systems and processes are effective.
- Identified any additional time-specific risks.

THIS APPROACH DOES MEAN THAT NOT ALL RISKS HAVE ASSURANCE, AND THERE ARE SOME CURRENT GAPS THAT HAVE NO ASSURANCE ACTIVITY. WE WILL ASSESS THE BEST WAY OF CLOSING THESE GAPS AS PART OF OUR PERFORMANCE ASSURANCE OPERATING PLAN DESIGN PROCESS. IT ALSO CHANGES THE FOCUS ON ASSURANCE, ADDRESSING MORE STRATEGIC, SYSTEMIC RISKS, WITH REDUCED FOCUS ON PROCESS COMPLIANCE.

2.2 SOURCES OF RETAIL RISKS

To ensure the Retail Risk Register is current and appropriately reflects the changes to risk profiles within the retail energy market, the Code Manager may identify new Retail Risks or make changes to existing Retail Risks based on:

Code Documents	• A comprehensive review of baselined code documents to identify the risks relating to parties' obligations captured within the obligations matrix, including engagement with REC SMEs as appropriate.
PAB Direction	• The PAB (and any of its regulatory and consumer representatives) has an active role in determining and refining Retail Risks, and the Code Manager will incorporate risks, or changes to risks that it identifies.
Party and/or Service Provider Behaviour	• The Code Manager will assess the impacts of Party and/or Service Provider behaviour as part of its risk and assurance activities. These may point to new and increasing risks, or demonstrate that existing risks are less relevant. • This will include updating risks following significant events or issues in the market.
Annual Assessments	• At a minimum the Retail Risks will be reviewed once a year, to identify if any new risks have arisen, or current risks need to change.
Change Requests	• As part of change impact assessments, the Code Manager will determine if any new Retail Risks arise, or if existing Retail Risks are changed or removed.
Performance Monitoring	• Based on the performance of REC Parties in relation to specific risk drivers, performance against risk drivers will be evaluated to understand whether additional risk drivers or Retail Risks are required

3. ANALYSING RETAIL RISKS

Each Retail Risk is recorded within the Retail Risk Register published on the REC Portal, which is categorised as a Category 3 document for change management and therefore administered by the Code Manager. The complete Retail Risk Register is available to the PAB.

One method of performance monitoring is establishing a detailed Risk Driver, although this is not appropriate for all risks. The table below sets out the information that is captured in relation to each Risk Driver within the Retail Risk Register to facilitate analysis of performance and inform the assessment of the Retail Risks.

Field	Description
Reference	A unique reference number for Retail Risks and Risk Drivers.
Retail Risk	One line explanation of the risk.
REC Obligations	References to specific REC schedules linked to the risk driver.
Types of Party	Types of Party for which this risk driver is relevant, and therefore may be assessed against it.
Types of consumers affected	Any particular customer groups that may be affected, including vulnerable customers, domestic, non-domestic, prepay customers, or other customer groups.
Related to customer vulnerability[1]	Yes / No field capturing if a risk driver relates to vulnerable customers, or groups more likely to contain vulnerable customers (e.g., prepay customers).
Related to effective competitive markets?	Yes / ~~no~~ No field capturing if the risk relates to market effectiveness. This could relate to potential barriers to entry, additional costs passed on to other participants or inappropriately obscuring information from competitors.
Threshold	Level determined by the PAB, above which, a Parties performance is deemed as unacceptable. The threshold is consistently applied across the market to each REC Party, and is defined by three components – maximum Normalised Risk Driver Score, period over which it is measured and minimum number of events occurring.
Pass criteria	Criteria for a process to be deemed successful.
Minor criteria	Criteria for a process to be deemed as an exception.
Major criteria	Criteria for a process to be deemed an exception, and the consumer harm may be more significant.

[1] The Code Manager uses the Ofgem definition of a vulnerable customer, which is defined as follows:
'A vulnerable consumer is defined as one who is:
- Significantly less able than a typical consumer to protect or represent their own interests; and/or
- Significantly more likely to experience detriment, or for that detriment to be more substantial.'

4. ASSESSING RETAIL RISKS

This section details how Retail Risks are measured. This is based on performance data, available from market sources, provided directly by parties or derived by the Code Manager. Risk measurements are updated on a monthly, quarterly, annual, or ad hoc basis as appropriate. Upon receipt of the available data, calculations are performed to measure the extent to which a Retail Risk is likely to materialise.

4.1 WHY DO RETAIL RISKS NEED TO BE ASSESSED?

Retail Risks need to be assessed in order to understand the performance of individual REC Parties, service providers and the market as a whole in order to identify where REC objectives are not being achieved resulting in customer detriment, with interventions required.

The measurement criteria may involve direct measures of compliance/success at defined stages of a process (e.g., analysis of market messages), performance reports produced by service providers or parties, and indirect measures of consequential outcomes. These are summarised within the monthly report to PAB on performance, which focuses on both Party and industry level performance, based on the type of Retail Risk and the Risk Driver.

Where there is an established measure the PAB may set thresholds for further action. Where this is relevant they are included in the risk register's supporting documentation.

Based on the number of passes, minors and majors (driven by factual datapoints) at a performance measure level, a risk score is calculated in respect of each Risk Driver.

Major instances have a higher risk score attributed to them than minors, leading to assurance intervention, including assessment activities where appropriate.

4.2 ANALYSIS AT RISK DRIVER LEVEL

We undertake analysis of Risk Driver scores to enhance the understanding of performance through three key activities:

- Comparing performance at Risk Driver level across Parties to understand how different Parties are meeting specific process requirements and whether issues are specific to a party or commonplace across the market. This highlights Parties with poorer performance against a specific requirement.
- Analysing direction of trend in performance at a Party level to focus on deterioration in individual Party performance. Trends are calculated based on performance in the previous measurement period, and serve as an indicator of how party performance is improving or deteriorating.
- Comparing performance to the thresholds set by the PAB. This also provides an opportunity for the PAB to increase performance expectations over time, by decreasing thresholds.

To aid comparison a 'normalised score' for each Risk Driver is calculated. This is the weighted proportion of instances where the Party did not meet the requirements of the measurement criteria based on the total instances that it could have, and the risk score is a relative indication of the extent to which the Party did not meet its specific obligation being measured. This approach means that larger Parties are not subject to additional assurance activities solely based on their size, and that assurance activities can be focused on the areas of greatest risk. This approach enables comparison of performance of a Party against its peers for a specific Risk Driver, analysis of trends in a Party's performance over time and performance in particular process areas across parties.

Further analysis and assessment for Parties is focused on those with poor performance, deteriorating performance or breaching PAB threshold. This will inform the subsequent selection of applicable PATs.

4.3 RESPONDING TO RISK DRIVER SCORES

For parties performing at the required level, no specific action will be required. The Code Manager will respond to high or increasing risk driver scores through application of one or more Performance Assurance Techniques (PATs) details in sections 6 – 11 of this document.

The Code Manager may use existing information to "whitelist" or adjust for known false positives or where a corrective plan is already in place. Specific details on how PATs would be applied across risk drivers and measurement criteria are detailed within this document.

4.4 DE MINIMIS SCORING

When assigning thresholds, there will be a de minimis applied. This will be applied where Parties have not had enough passes, majors and minors overall, to give a fair result which reflects their true performance. Their score maybe distorted due to the low population being used. Where this is required, Performance Assurance Techniques (PATs) will not be immediately applied. Instead, there will be ongoing monitoring to ensure that PATs are applied as and when a sufficient population is available to be assessed and this shows poor performance.

4.5 DATA CLEANSE

Overview

Maintaining accurate data is a key responsibility under the REC, baselined in Schedule 24 – Switching Data Management, as lack of data quality can impact other Parties and consumers leading to negative outcomes and poor consumer experiences. As a result, Data Cleanse activities are an important Performance Assurance requirement.

In some cases, Data Cleanse items cannot be cleansed to zero, and when switching occurs Energy Suppliers can acquire customers with data issues; these issues will be considered when the Code Manager recommends the actions and targets for Data Cleanse activities.

Prior to proposing Data Cleanse activities, the Code Manager will seek input from industry; this may include relevant forums such as the REC Issues group, Performance Assurance Webinar, PAB, and wider industry groups. Data Cleanse activities involve implementing a combination of PATs, which are outlined below for ease of reference.

Application of PATs

Based on the feedback from Industry, the Code Manager will propose a **Cross Industry Monitoring PAT** in the form of a Data Cleanse. This PAT will include the report description, impacted Parties, the rationale for inclusion, and where applicable further guidance and specific targets for Parties.

There are different Data Cleanse activities that the Code Manager may recommend, depending on the level of risk, as outlined below:

~~Maintaining accurate data is a key responsibility under the REC, as well as key way in which the actions of one organisation can have negative impacts on other market participants, or consumers. As a result a key Performance Assurance activity is data cleanse. We recognise that many data cleanse items cannot be cleansed to zero, and that when switching occurs Energy Suppliers can acquire customers with data issues. As a result our methodology for data cleanse is to track specified metrics with different approaches based on the assessment of risk relating to the data items. These approaches are:~~

Approach	Description
Sprint	We set data cleanse targets, approved by the PAB, for Parties to deliver. ~~-~~If these targets are not met by an individual Party we apply relevant PATs, agreeing the approach with PAB as appropriate. A sprint approach is followed in order to focus effort across the market on prioritised issues and to manage the risk of such issues being transferred on switching.
Track	We share these data cleanse reports with Parties, with the expectation that they improve data where possible. ~~–~~If performance dramatically changes we may engage with relevant Parties to understand more, but don't envisage applying remediation or escalation PATs ~~(see below)~~.
Watching Brief	We continue to run these reports and share them with Parties, but are not actively considering them. ~~–~~This is most commonly used where reasonable efforts to cleanse data have been taken, but we want to be alerted if an event in the market

	causes data issues. We do not expect Parties to actively cleanse these, but do expect day to day operational processes to continue.

Further information on the Data Cleanse reporting process can be found in the **Data Cleanse Report Guidance** document on the REC Portal.

Where Parties fail to meet Data Cleanse Sprint targets, the Code Manager may propose further PATs to PAB. Typically, this will include an *Assessment PAT*, such as an **Enquiry PAT**, requiring the Party to explain why they have failed to meet their Data Cleanse Sprint requirements. Where the Code Manager requires the Party to make further improvements, a *Remediation PAT* may be proposed, such as an **Action Plan PAT**, to outline the specific actions that the Party is required to take within a specified timeframe. Finally, if the Code Manager is still not satisfied with the Party's progress, the Code Manager may propose a further *Escalation PAT* to incentivise performance and protect the market.

Further Data Sprint Considerations

1. The REC Manager will consult with industry to understand both the benefit and cost of proposed Data Cleanse items before requesting approval from PAB.
2. Data Cleanse reports are provided via the REC Portal but will only be visible privately to the Party concerned and the Code Manager. Through access to the REC Portal, Parties can provide updates on progress completing actions and request exemptions.
3. The Code Manager will publish the start date, end date, and specific targets for each Data Sprint to Parties in advance of the Sprint commencing.

RACI matrix setting out delegated authority for data cleanse activities			
	PAB	Code Manager	REC Parties
Determine focus and content for Data Cleanse sprints	A	R	C
Approve specific Data Cleanse content and targets	R	C	I
Provide guidance on Data Cleanse methodology	A	R	C
Approve Data Cleanse exemptions based on agreed methodology		R	C

5. PERFORMANCE ASSURANCE TECHNIQUES (PATS)

5.1 BACKGROUND

Performance Assurance Techniques are used to drive good performance in retail energy markets. Our approach focuses assurance activities on the highest priority areas, with the aspiration of reducing the burden of compliance for those that perform well. To enable this, we have two categories of assurance:

Baseline techniques – these apply to all REC Parties who operate in the market. The requirements for this baseline which require direct interaction with the Code Manager are predominantly preventive and kept to a minimum. Detective baseline activities will include regular monitoring of relevant retail risks. The Maintenance of Qualification (MoQ) process is the key mechanism for baseline assessments, although in specific instances peer comparisons may apply to all Parties. The details of these requirements are communicated in advance through the Performance Assurance Operating Plan.

Risk focused techniques - these techniques are applied based on the results of our monthly data driven risk assessment. The Code Manager will identify the appropriate technique to address the risk, based on the suite of PATs described in this document. This will involve traditional assessments of a specific Party, as well as techniques focused on understanding the root cause of issues, or incentivising sections of the market.

Some of these techniques may be applied by the Code Manager automatically, with others requiring PAB input and approval. Throughout this document, the following badges will be used to identify which category the technique falls into.

Baseline Techniques	Techniques applied based on info	Code Manager Delegated Authority	PAB approval required to apply the technique
			
Applied to all REC Parties as standard	Applied as required	Applied by the Code Manager without PAB request	Not automatically applied by the Code Manager

Throughout the document we will also identify where techniques apply to Parties, non-Party Service Users and REC Service Providers. This will be clearly labelled at the top of each page alongside the above badges.

5.2 METHODOLOGY FOR RISK MANAGEMENT DETERMINATIONS

Three of the key functions of the PAB, as set out in section 3 of the Performance Assurance Schedule are making determinations on:

1. Revisions to the Retail Risk Register.
2. The application of PATs in order to mitigate the risks to REC Service Users or REC Service Providers that may result from non-compliance.
3. Breaches of the Code and Events of Default.

We interpret that point 2 can also cover risks to consumers, including Retail Risks and other risks, and point 3 covers both risks and issues (including risks that have crystallised).

Risk Management Determinations are defined within Section 7 of the Performance Assurance Schedule.

The PAB shall make Risk Management Determinations based on the information it has in three ways:

1. Proactively, based on its assessment of risk to apply baseline techniques, informed by the Retail Risk Register. These will be set out in the Performance Assurance Operating Plan.
2. Based on information received, at which point the Code Manager or PAB can apply PATs, based on the delegated framework and decision making authority established in this document. The risk and Risk Management Determination will be clearly communicated to the relevant organisation.
3. Based on risk data, as set out below, although these determinations may not always result in PATs.~~.~~

~~3.~~

5.3 USING DATA TO MAKE RISK MANAGEMENT DETERMINATIONS

The approach to identifying and assessing risks is included in the Performance Assurance Methodology (PAM). The Code Manager will use the PAM to monitor risks and risk drivers evaluating these, in most cases, on a monthly basis at the Code Manager Data Review session. Thresholds are defined by the PAB for the majority of Risk Drivers and where the measurement of a Risk Driver exceeds the defined threshold the Code Manager will act and apply PATs. The Code Manager may also apply PATs in other circumstances, notably where Risk Drivers are increasingly significantly and rapidly or where a specific Party's Risk Score is significantly out of line with market-wide performance. These decisions constitute Risk Management Determinations.

Risk Thresholds consider three factors:

- Risk Score Expectation / Limit – the risk score value over which performance is considered to have met the threshold (higher scores indicate lower performance).

- Trend Period: The period over which the risk score is measured. This can be monthly or multiple months, with longer trend periods allowing for some short-term variance in performance with action taken when sustained issues are noted.
- Minimum activity level: The minimum number of activities measured by the risk driver that have to have occurred in a month for the threshold to be applied. This is used to avoid thresholds being overly sensitive to very low volumes of activities for a specific Party.

The way the Code Manager responds is dependent on the type of metric which indicated a risk. These can be classified into four groups:

- Compliance metrics linked to Party charges.
- Compliance metrics not linked to Party charges.
- Outcome metrics.
- Market wide outcome metrics, i.e., ones that relate to several different market participants.

The Code Manager will use the risk data in these areas to identify the most appropriate PATs to apply. In doing so the Code Manager will take into account the following factors:

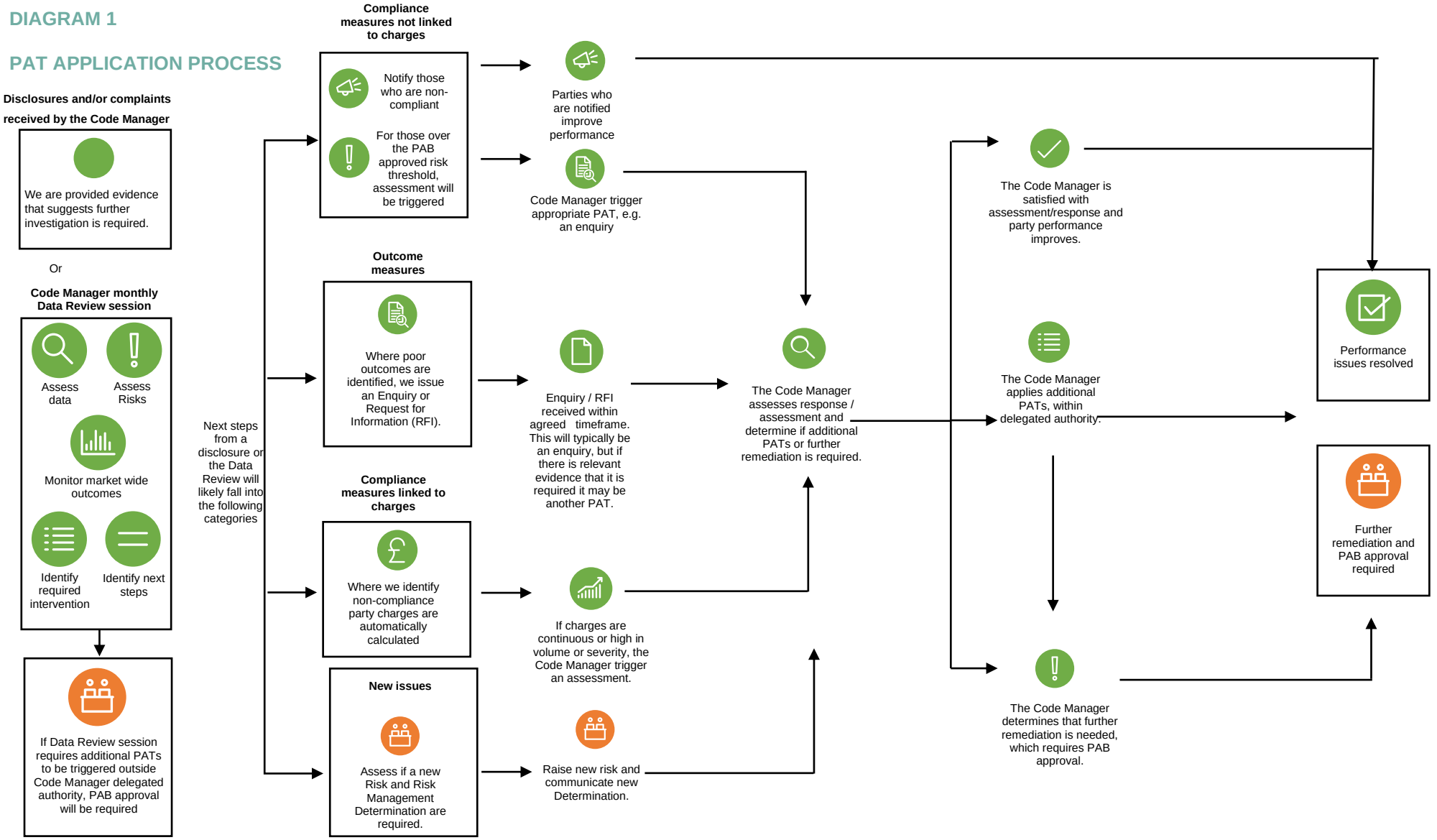
- Whether existing PATs are already active for the Risk Driver, or for other Risk Drivers under the same Retail Risk.
- The history of PATs applied for that Party and Risk Driver, and other Risk Drivers under the same Retail Risk.
- The number and nature of Risk Drivers exceeding threshold or otherwise triggering the application of PATs - pervasive poor performance may require different approaches to remediation.
- Existing knowledge about that Party's operations and performance based on information provided by the Party, OAMs and from application of previous PATs. This includes whether the Party is under CME.
- Other contextual information about that Party – for example if it has recently acted as a Supplier of Last Resort (SoLR), has engaged in a significant transaction to acquire another Party's business / customers or has notified the Code Manager via the Change or Incident Notification.
- The nature of the specific Risk Driver (including whether it is outcome or compliance based) and the associated Retail Risk – for example whether detriment arising from the performance impacts Customers or Parties.
- The priority the risk has been assigned by the PAB. This will be the key consideration in areas where timely, relevant performance data is not available, or waiting until failures occur before intervening is inappropriate, e.g., information security.
- Consideration of the overall profile of Party performance. For example, if all Parties are performing significantly worse than the performance expectation, a market wide approach may

be more appropriate, whereas if individual Parties are outliers targeted interventions may be more appropriate.

Diagram 1 on the following page illustrates the process of using data and disclosures made to the Code Manager to inform Risk Management Determinations and apply PATs in further detail.

DIAGRAM 1

PAT APPLICATION PROCESS

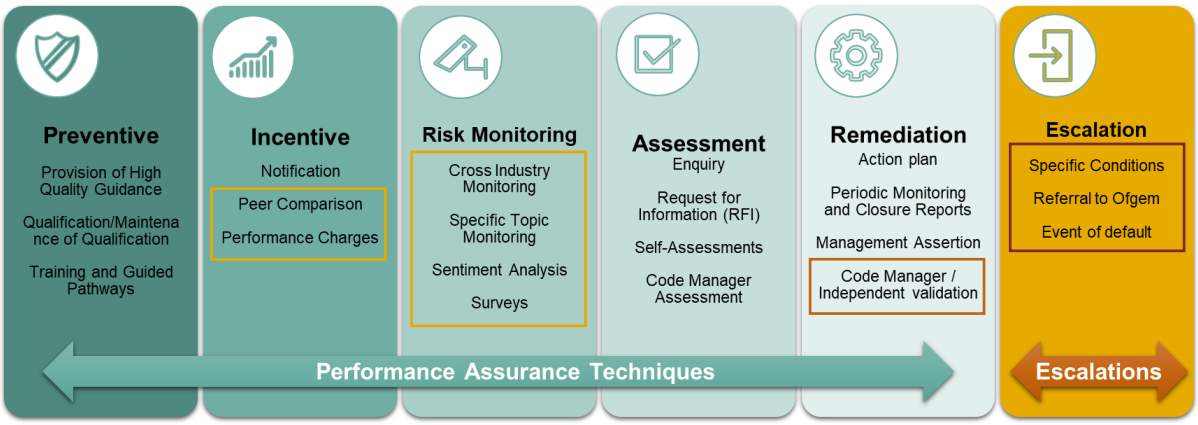


5.4 GOVERNANCE OF PATS

There are some techniques that require additional governance and oversight to apply. This will generally be on occasions where escalation is required, and judgement is needed to apply these techniques. The techniques highlighted below are those which require PAB oversight and approval to apply the technique.

Some of these techniques will need the PAB to approve how the techniques are used and the parameters for their use, which the Code Manager can then apply. For example, the PAB will govern the use of performance charges and set the thresholds for when charges are applied. Once these thresholds have been set, charges can be applied within the agreed parameters. These techniques are highlighted below in yellow.

For other techniques, the PAB must approve the use of the technique in order for them to be applied. These are more serious interventions and therefore an enhanced level of PAB approval is required. These techniques are highlighted below in orange and red. Whilst the techniques highlighted in orange focus on remediation, the ones in red are significant escalation techniques.



Parties will be provided with reasonable notice of the application of PATs and any associated costs, except in the case of material issues which require more immediate intervention. Further details on this are included in section 5.5.

The table below outlines key activities related to PATs where additional governance and oversight is required.

PAT Related Activity	Governance and oversight
Introducing a new PAT	A REC change request. This includes consultation with Ofgem and the industry.
Introducing a new performance charge	A REC change request. This includes consultation with Ofgem and the industry.

PAT Related Activity	Governance and oversight
Applying an existing PAT in a new way	PAB decision to approve the use of the technique, with affected Parties notified via the REC Portal
Applying an existing PAT	Code Manager decision, based on observable data, subject to PAB approval where required.

5.5 COMMUNICATING WITH PARTIES AND APPLYING TECHNIQUES WHEN A POTENTIAL PROBLEM IS IDENTIFIED

The Code Manager Data Review session is the forum for the Code Manager to assess risks and identify potential performance issues. This is held on monthly to review the insights presented within the Performance Assurance Dashboards. At this session, the Code Manager reviews the instances of REC Parties breaching thresholds set by PAB and any other anomalies presented within the Performance Assurance data, to determine appropriate course of action. The Operational Account Managers are engaged during this process to help consider contextual information when reviewing the data.

Additionally, as the market is evolving, there may be times when the Code Manager is made aware of issues which are significant but are considered for the first time. These may not currently be in the Retail Risk Register, but it is important that these are acted upon. In these instances, the Code Manager can take action to understand the issue, such as making Enquiries. However, they will consult with the PAB on any further action, and this may include the application of further PATs.

A transparent Performance Assurance approach allows Parties to respond positively to assurance and minimises disruption on Parties requires clear communication. To achieve this transparency the Code Manager will adhere to a set of principles when applying PATs as outlined below. The principles include:

- Notify first, allowing the Party to proactively investigate and fix potential issues.
- Take a two-tier approach to PAT application wherein urgent matters get acted upon monthly, whilst other potential issues are batched up for quarterly issue of PATs, and where appropriate, utilise forum such as REC Issues Group (RIG) to consult with the industry.
- Parties are provided the Risk Management Determination which sets out the reason why PATs are applied.
- Each PAT will have a defined start date. Depending on the nature of the PAT it will also either have an end date, or defined exit criteria which when met will result in the PAT no longer applying. This information will enable Parties to understand what needs to be achieved in order to reach compliance and prepare a response within the allocated time frame. Where the PAT requires submission of evidence these will have deadlines for submission.

- There is a lead time before techniques are applied. Therefore, if a REC Party is in the process of having an assessment, high risk scores again do not automatically trigger another assessment.
- Parties often need time to improve performance. Therefore, if an action plan is in place or other remediation technique, this will be monitored and if the Party continues to be identified in risk data, this will not automatically trigger another assessment.
- Where performance charges exist, the same poor performance is not penalised twice.

5.6 APPLYING TECHNIQUES WHEN ESCALATION IS REQUIRED

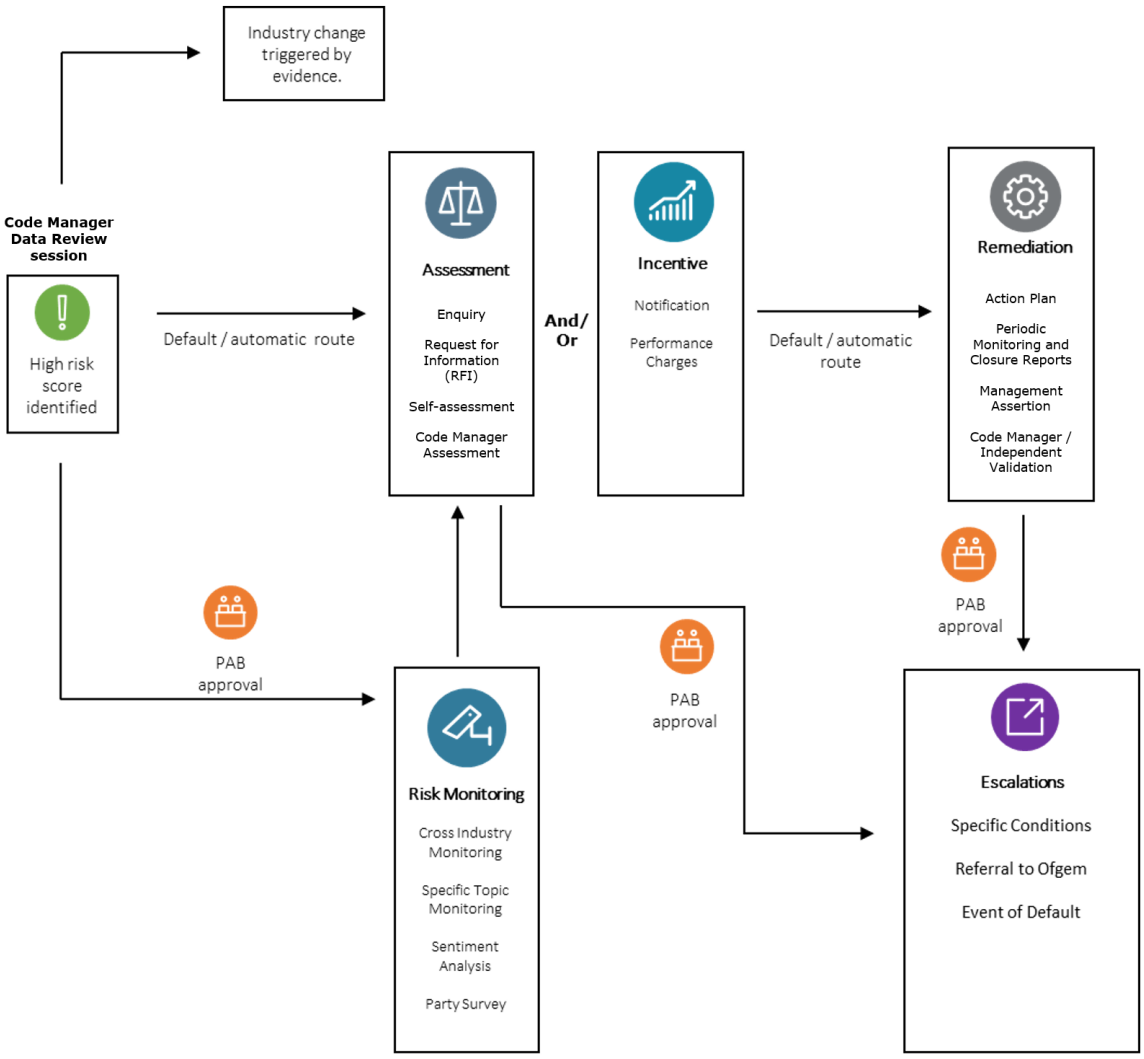
At the Code Manager Data Review session, the Code Manager will also assess when performance issues and applying PATs need to be escalated. There are three main routes for escalation:

- Code Manager determines that additional PATs need to be triggered, which are outside the Code Manager's delegated authority and require PAB approval.
- Code Manager applied PATs have not resolved performance issues and further escalation techniques are needed, which require PAB approval.
- Code Manager determines that the evidence suggests that an industry change is needed, rather than individual PATs being applied to resolve the problem.

The following diagram (Diagram 2) illustrates the escalation process in more detail.

DIAGRAM 2

PAT ESCALATION PROCESS FOR PERSISTENT POOR PERFORMANCE



5.7 APPLYING TECHNIQUES TO CODE MANAGER BODIES AND SERVICE PROVIDERS

The Code Manager's performance assurance role also covers the REC Technical Service (RTS) and REC Professional Service (RPS), as well as other Service Providers. These organisations have a different role, often with no comparable peers. Like Parties, PATs can either be applied directly to address risk, or in response to risk measures. There are though some differences in the way PATs are applied to these organisations. This is summarised below.

	Parties	RPS / RTS	REC Service Providers
Focus of assurance	Predominantly in response to poor performance identified through the risk process.	Unlike the use of the PATs with REC Parties, we expect the focus to be on cyclical assessments rather than in response to performance data.	Assurance is a combination of cyclical assessment and responses to performance data.
How this is scoped	Specific work is performed based on the areas of poor performance.	A universe of obligations has been developed which focuses on risk, with the most critical assessed each year, and the less critical assessed as part of a rolling three year plan.	This will include inputs from meeting with the Service Provider, communications sessions they hold, information from other market participants and input from RECCo.
In addition to validating with the Party or REC Service Provider, how this is reported	Findings and themes are reported monthly to the PAB, with aggregate findings and how these should be responded to by REC governing bodies in the REC Performance Assurance Annual Report.	Findings from the cyclical assessments are included in reports to PAB and the REC Performance Assurance Annual Report.	Findings from the cyclical assessments are included in reports to PAB and the REC Performance Assurance Annual Report.

When applying PATs, the organisation that has Code obligations is responsible for providing us information, access and engaging with the portal. For example, Parties may have obligations relating to "Licence Lite" suppliers or retail data agents. Services may be provided by subcontractors; however, our assurance will focus on the REC Service Provider.





6. PREVENTIVE TECHNIQUES

Provision of High Quality Guidance

Qualification/ Maintenance of Qualification

Training and Guided Pathways

6. PREVENTIVE TECHNIQUES



6.1 PROVISION OF HIGH-QUALITY GUIDANCE

Overview

High quality guidance (e.g., good practice guides) is provided by the Code Manager (including REC Professional Services, Technical Services and Performance Assurance providers) to all Parties and will act as preventive measure to stop operational or process issues from occurring and reoccurring in the future. The guidance is digitalised and available through the REC Portal. The Code Manager will oversee the adoption of guidance materials and confirm that Parties are utilising the resources available to them.

How this will be used

High quality guidance is a baseline technique and will be used to educate Parties on areas where they require support to prevent issues from either occurring or reoccurring in the future.

Controls in place over its use

1. Guidance will be published on the REC Portal so that it is easy for Parties to access.
2. Prior to any updated versions of guidance being published, the Code Manager will conduct stakeholder engagement with Parties to gather feedback prior to release.

RACI matrix setting out delegated authority for applying or changing techniques

	PAB	Code Manager	REC Parties
Monitors the adoption of guidance and makes recommendations for changes as appropriate.	I	R	I
Develops and updates guidance.	C or I (depending on the guidance)	R / A	
Approves guidance materials.	R / A (some not all)	C	I
Informed when changes or updates are made.	A	R	I

6.2 QUALIFICATION / MAINTENANCE OF QUALIFICATION



Overview

To operate in the market all Parties must complete the qualification process. This includes entry as a Party and gaining access to specific services as a REC Service User.

This assesses whether applicants to be Parties meet the market standards from the outset and there is clear and documented evidence that Parties have the appropriate systems, processes, controls and security in place to meet this standard. The initial qualification process involves four key assessments, a business solution assessment, an assessment of the internal testing completed by the applicant, an information security assessment and external testing with DCC and the Code Manager. The transition to Marketwide Half Hourly Settlement (MHHS) may introduce additional external testing requirements with the Data Integration Platform (DIP) manager.

REC Service Users are assessed specifically against information security requirements, so that risks related to the access to customer data that they are granted are understood and mitigated.

To maintain qualification, Parties will have to complete a Maintenance of Qualification process which is required annually, or may be required following the disclosure of a material event, such as a change or failure, that has occurred or is anticipated.

How this will be used

Qualification is a preventive technique and is used to assess the capability of applicants to fulfil their role in the market. Maintenance of Qualification is used as the key touchpoints with Parties who are not identified for further PATs through the risk assessment process. It therefore includes the following:

1. Annual attestation by management, in the form of a self-assessment return and Director (or duly authorised delegate) statement, in relation to their processes, systems and resources.
2. Periodic assessment of ongoing compliance with information security requirements.
3. Gathering information on any specific thematic investigations, as described in the Performance Assurance Operating Plan (PAOP).

Completion of this process may result in Parties qualified for a market role or qualified but with specific conditions in place. For new entrants, qualification could also be rejected with reasons provided for this decision.

Controls in place over its use

1. The details of the Maintenance of Qualification process are defined in the REC Maintenance of Qualification Guidance.
2. The details of the qualification process are published and made available online through the REC Portal, in both the publicly available space as well as the area available via login,

including the information required, assessment steps and the criteria against which applicants are assessed against.

3. As set out in the Qualification and Maintenance Schedule, entry decisions are made by the Code Manager, with escalation and appeal decisions made by the PAB as required.

RACI matrix setting out delegated authority for applying or changing techniques			
	PAB	Code Manager	REC Parties
Update and develop forms to improve comprehension.	I	R / A	C / I
Change the methods, criteria or data collection as part of this process.	A	R	C / I
Update communication mechanisms between Code Manager entities and / or other Codes.	I	R / A	

6.3 TRAINING AND GUIDED PATHWAYS



Overview

Training materials and guided pathways (e.g., compliance training) are provided by the Code Manager to all Parties and will act as a baseline and preventive measure to stop operational / process issues from occurring or reoccurring in the future. The Code Manager will monitor that Parties are utilising the training resources available to them, using the analytics capabilities of the REC Portal.

How this will be used

Training and guided pathways will be used to assess Parties on areas where they require support to prevent issues from either occurring or reoccurring in the future.

Controls in place over its use

1. Training may include a test on completion to validate and confirm learning from the training.

RACI matrix setting out delegated authority for applying or changing techniques			
	PAB	Code Manager*	REC Parties
Update and develop guidance.	A	R	I

*In this instance the roles of the Code Manager are discharged by the various teams, not just the Performance Assurance team, depending on the specific guidance document.





7. INCENTIVE TECHNIQUES

Notification

Peer Comparison

Performance Charges

7. INCENTIVE TECHNIQUES



7.1 NOTIFICATION

Overview

Where our risk assessment activities identify instances of non-compliance with the REC or poor customer outcomes, Parties will be notified of this so that they can understand where they need to improve their performance before any further action is taken by the Code Manager. This acts as an incentive to resolve poor performance, and may even be applied where they have not yet passed the threshold requiring Code Manager intervention.

How this will be used

The Code Manager will use notifications, through the REC Portal dashboard, as a form of incentive to notify Parties when they are not being compliant with the Code or are at risk of poor customer outcomes. This should allow Parties to resolve issues themselves, and reduce the likelihood of repeated instances of the same issue. It may also indicate to Parties opportunities to enhance the Code, for example by raising change requests where non-compliance is identified yet this does not impact customer outcomes.

Controls in place over its use

1. Notifications are based on the market monitoring we perform as part of our risk assessment work. They are therefore only notifications of Risk Driver above threshold.

RACI matrix setting out delegated authority for applying or changing techniques			
	PAB	Code Manager	REC Parties
Changes to the risk measures we monitor.	R	A	C / I
Change to the mechanism to notify (e.g., updates to the specific text of the notification).		R / A	

7.2 PEER COMPARISON



Overview

In response to specific cross industry risks the Code Manager may implement a peer comparison based on Party performance data. The Code Manager will implement peer comparison to act as an incentive for Parties to improve performance. The data for the peer comparison is shared with the Performance Assurance Board by the Code Manager so they can have visibility over Party performance. This data can be displayed on the REC Portal so that Parties can compare themselves to their peers and assess their performance The exact set of data, or who constitute peers, will be defined to address the specific industry risk.

How this will be used

Peer comparison will be used to incentivise Parties on objective, measurable performance criteria. The indicators used for the peer comparison will be made clear to all Parties, with the intention that competition amongst peers will provide a meaningful incentive to achieve greater performance. Peer comparisons will be provided to both affected Parties and the PAB, with some peer comparisons published on the public internet.

Controls in place over its use

1. The criteria for comparison, and the timeframe the comparison will be active for, are approved by the PAB and published by the Code Manager. This will include what information is visible to Parties (e.g., they may be provided their performance against anonymised peers, have full visibility of peer group performance, or even have their performance published externally).
2. The format of the peer comparison is approved before use by the PAB.
3. Each peer comparison which the Code Manager designs and are intended to be published online will require PAB approval.

RACI matrix setting out delegated authority for applying or changing techniques			
	PAB	Code Manager	REC Parties
Designing and implementing the peer comparison.	A	R	I
Approving changes to the peer comparison.	R / A	C	I
Extending the use of the peer comparison, e.g., for another year.	R / A	C	I

7.3 PERFORMANCE CHARGES



Overview

The Code Manager will monitor Service Providers performance against certain function requirements, as may be set out in the REC. As with other contracts, the Service Provider may be incentivised to deliver these requirements, or to compensate REC Parties where they have not delivered them, through the application of specific performance related charges. In in similar way, market activities will also be monitored. Where a REC Party / Service User fails to meet a pre-agreed benchmark standard, they may be liable for a performance charge. This performance charge will be identified by the Code Manager with recovery of the financial charge from the Party administered by RECCo.

RECCo will invoice the Party/Service User for the financial charge on notification by the Code Manager and the invoice will be payable according to the credit terms set by the RECCo Board. For Service Providers, RECCo will reduce the Performance Charge from the amount that would otherwise be payable to a REC Service Provider.

How this will be used

Performance charges will be used to incentivise Parties on objective, measurable performance criteria. The intention is not to use these charges to offset revenue costs, but as a technique to be used to incentivise improved performance for high priority risks.

Controls in place over its use

1. The criteria for applying charges are defined and consulted on in advance of their application and publication. This will take the form of a change proposal. Depending on the nature of the charge this could include caps and collars, to avoid either the administrative impact of very small charges, or excessive charges, e.g., where a Party system error results in many penalty events.
2. Charge rates are subject to consultation through a change proposal before use, with rates approved by the PAB prior to being included in the change proposal.
3. If charge rates are recommended to change, these changes will be consulted on prior to approval, through a change proposal.
4. The PAB can suspend charges for the market, as appropriate and in consultation with Parties.
5. The Code Manager will report on the aggregate use of charges as part of its annual report.

RACI matrix setting out delegated authority for applying or changing techniques			
	PAB	Code Manager	REC Parties
Changes to the criteria which trigger charges.	R	A	C

Changes to the value of charges.	R	A	C
Changes to the mechanisms by which charges are communicated or administered.	R	A	I





8. RISK MONITORING TECHNIQUES

Cross Industry Monitoring

Specific Topic Monitoring

Sentiment Analysis

Surveys

8. RISK MONITORING TECHNIQUES

8.1 CROSS INDUSTRY MONITORING



Should we identify issues that affect the entire industry, or large groups of Parties, we can use cross industry monitoring to gain greater insight into the causes of, and potential solutions to, industry wide issues. This will involve regular monitoring, usually involving detailed analytics, above and beyond our risk assessment work. This is distinct from peer comparison, as this information will not be published directly to Parties or the public, although our overall conclusions may be.

How this will be used

Cross industry monitoring will be used in response to identified or anticipated issues that affect groups of Parties. For example, this could be used on occasions where there are multiple complaints of the same nature, or when there is a system or process issue that is affecting multiple Parties. It could also be used to monitor larger system and process changes, to assess the success of the change and manage any changes that occur post-implementation that may have consumer impacts. This will include instances where entire groups of Parties have failed to meet the expected standard, as well as in advance of and following a change to identify if the change has had the intended effect.

Controls in place over its use

1. The criteria for cross industry monitoring are defined and approved by the PAB in advance of their application. This includes the specific question that this technique is being used to address.
2. Parties that are identified for monitoring are notified with the reason for monitoring explained, with a follow up notification detailing the results. This will be provided in an aggregated or anonymised form, to avoid this appearing to be peer comparison.
3. The Code Manager will report on risks identified through cross industry monitoring as part of its annual report, or interim reporting as suitable, focusing on general trends rather than individual findings.

RACI matrix setting out delegated authority for applying or changing techniques			
	PAB	Code Manager	REC Parties
Designing and implementing the cross-industry monitoring.	A	R	I
Approving changes to the cross-industry monitoring.	R / A	C	I
Extending the use of the cross-industry	R / A	C	I

monitoring, e.g., for another year.			

8.2 SPECIFIC TOPIC MONITORING



Overview

In contrast to cross industry monitoring, specific topic monitoring focuses on small groups or individual Parties and therefore focuses on a specific area of monitoring. For example, Parties with specific conditions (e.g., limits on the number of new customers acquired), may have these conditions monitored, or specific monitoring may be put in place following improvement activity.

This will be performed by the Code Manager in order to observe the behaviours of specific groups of Parties i.e., Suppliers, DNOs, MEMs, etc.). If an issue is observed or brought to the attention of the Code Manager, they are then able to intervene and develop corrective measures.

How this will be used

The Code Manager will use specific topic monitoring as a method of monitoring risk across the market. The technique will be used when a topic is identified as a problem or risk but is not necessarily attributed to individual Party performance. This could be when something new is launched in the market and the Code Manager wants to monitor the impact of this, or if there is a problem that all Parties are experiencing, and further investigation is required to find out the cause of this problem.

This may involve monitoring based on data from central services, but it could also involve Parties regularly providing data for us to fulfil this monitoring role.

Controls in place over its use

1. The criteria for specific topic monitoring are defined and approved by the PAB in advance of their application (although the specific topic to be monitored may only be identified subsequently).
2. Parties that are identified for monitoring are notified with the reason for monitoring explained, with a follow up notification detailing the results.
3. The Code Manager will report on risks identified through topic monitoring as part of its annual report, focusing on general trends rather than individual findings.

RACI matrix setting out delegated authority for applying or changing techniques			
	PAB	Code Manager	REC Parties
Designing and implementing the specific topic monitoring.	A	R	I
Approving changes to the specific topic monitoring.	R / A	C	I

8.3 SENTIMENT ANALYSIS



Sentiment analysis refers to the process of using natural language processing techniques to mine text to identify and extract subjective information in data. This can be used as an assurance technique, for example analysing social media such as Twitter and Facebook, to gauge public opinion, monitor reputation and understand customer experiences.

How this will be used

This technique will only be used to assess a specific concern, for example if we identify a high incidence of poor outcomes, and will be used as an appropriate mechanism to assess customer impact.

It will be used as a risk monitoring technique to provide greater insight into the causes and potential solutions to specific performance issues. This will be used to supplement the analysis made on customer complaints data available to Code Manager.

Controls in place over its use

1. The parameters for sentiment analysis (i.e., what platform will be used for the analysis, the frequency of analysis, the end date, the intended benefits of this analysis etc.) will be set by the Code Manager and approved by the PAB.
2. Sentiment analysis will be used alongside other risk monitoring techniques rather than used in isolation, to avoid a skewed perception based on sentiment analysis alone.

RACI matrix setting out delegated authority for applying or changing techniques			
	PAB	Code Manager	REC Parties
New or amended sentiment analyses.	R	A	I
Extension of sentiment analysis past its agreed end date.	R	A	I

8.4 SURVEYS



Overview

Similar to cross industry monitoring, there may be scenarios where we identify poor customer or Party outcomes, but our risk assessment does not necessarily identify this is likely to be caused by a specific Party. In these instances, surveys can be used to gather feedback from Parties. For example, they could be used to assess how a Code or system change has affected Parties, or if actions taken by central services have resolved issues faced by Parties or Service Providers.

How this will be used

Surveys will be used by the Code Manager in order to understand both the performance of Parties and the root causes of known issues. They will be used to gather feedback on performance, with each survey having a defined frequency and results compared against previous surveys to determine trends.

Controls in place over its use

1. The Code Manager will determine the frequency of surveys and will be and set a standard expectation for completion (e.g., a standard timeframe for completion, a minimum number of engagements for Parties per year), which will require PAB approval.
2. The Code Manager will determine how survey feedback is used and communicated to Parties.

RACI matrix setting out delegated authority for applying or changing techniques			
	PAB	Code Manager	REC Parties
Designing and implementing a new survey, or changing or rerunning an existing one.	A	R	I





9. ASSESSMENT TECHNIQUES

Enquiry

Request for Information (RFI)

Self-Assessment

Code Manager Assessment

9. ASSESSMENT TECHNIQUES



REC Parties, non-Party Service Users and Service Providers

9.1 ENQUIRY

Our risk assessment process tracks both compliance measures, which directly relate to specific Code requirements, and outcome measures, which indicate a poor customer outcome but may not indicate the exact Code requirement that has not been met. For example, a slow resolution of an erroneous transfer is a poor outcome, but may be due to issues at one of many process steps. Whenever we identify a potential issue, we first get in touch with the Party to understand any potential causes. This is because we understand there may be factors, we are not aware of that we should take into account when interpreting the data. The Code Manager will apply the Enquiry PAT where we are asking for information so that we can understand this potential issue better.

How this will be used

Enquiry PATs will be used as a form of information gathering to validate the insights from the data analysed or issues and concerns reported to the Code Manager. This will help us understand whether there may be other contributing factors, beyond a Party's control, that may impact their performance.

Depending on the information received, further assessment, remediation or escalation activities may be triggered.

Controls in place over its use

1. There will always be a defined due date for Enquiries.
2. The number of Enquiries requested, and the nature of these Enquiries are reviewed by the Code Manager on a quarterly basis to make sure the use is proportionate.
3. Parties who fail to respond to Enquiries will be reported to the PAB.
4. Enquiries will involve a REC Portal request, so that they can be tracked, but they could be completed by other means, e.g., by phone call. The REC Portal request will be completed after this communication, so that organisations understand that the Enquiry has been completed.

RACI matrix setting out delegated authority for applying or changing techniques			
	PAB	Code Manager	REC Parties
Changes to the expected timescales for Parties to respond to Enquiries.	A	R	C / I

9.2 INFORMATION REQUEST (IR)



REC Parties, non-Party Service Users and Service Providers

Overview

Similar to Enquiry PATs, when our risk measures or whistleblowing indicate potential issues with performance, or to support PAB deep dives, information will be requested by the Code Manager in order to gain a more detailed understanding of what happened (e.g., how did it happen / why did it happen). If the Party does not provide sufficient information, the Code Manager will take further action using additional assurance techniques.

How this will be used

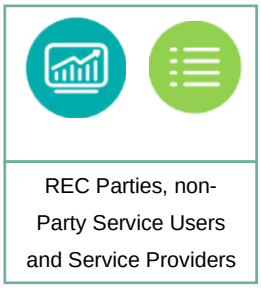
An Information Request (IR) will be used as a form of assessment to gain an understanding of why certain procedures / operations went wrong, and will also be used as part of thematic investigations to determine trends with under performance and identify how the cause of these issues can be resolved. Depending on the information received, further assessment, remediation or escalation activities may be triggered.

Controls in place over its use

1. There will always be a defined due date for IRs, as well as standard timescales for when IRs need to be completed.
2. ~~The number of IRs requested and the nature of these IRs is reviewed by the Code Manager on a monthly basis to make sure the use is proportionate.~~ The number of IRs requested, and the nature of these IRs, are reviewed by the Code Manager when proposed. PAB are notified of these IRs, and may challenge their application to ensure their use is proportionate.
3. Parties who fail to answer requests for information will be reported to the PAB.
4. IRs will involve a REC Portal request, so that they can be tracked, but they could be completed by other means, e.g., by phone call. The REC Portal request will be completed after this communication, so that organisations understand that the IR has been completed.

RACI matrix setting out delegated authority for applying or changing techniques			
	PAB	Code Manager	REC Parties
Changes to the expected timescales for Parties to respond to IRs.	A	R	C / I

9.3 SELF-ASSESSMENT



REC Parties, non-Party Service Users and Service Providers

Overview

Self-assessments are conducted by Parties to demonstrate they understand and meet their REC obligations. The Code Manager may request a Party to complete a self-assessment to:

- Assure PAB that the Party is complying with the Code.
- Assess whether a Party is taking appropriate measures to resolve issues and prevent reoccurrence where it has not met market standards.

These are separate to routine self-assessments that all Parties will need to provide as part of the Maintenance of Qualification process.

How this will be used

Self-assessments will be used to ascertain which areas of the business, if any, require improvement. Should the Code Manager determine further action is required a remediation technique, or further assessment, will be triggered. This will enable problematic areas to be mitigated and subsequently optimise performance.

Controls in place over its use

1. Self-assessments are focused on an identified breach / non-compliance with market standards, as identified through the risk assessment process or another Performance Assurance Technique.
2. Formal deadlines for Parties to provide their self-assessments are communicated, alongside the request for self-assessment.
3. Once the Code Manager has examined the self-assessment report they will confirm to the organisation that this has concluded and if any further action is required.
4. The Code Manager reports to the PAB on Parties which fail to complete self –assessments in line with the deadlines.

RACI matrix setting out delegated authority for applying or changing techniques			
	PAB	Code Manager	REC Parties
Updates to the specific areas for self-assessment.	I	R / A	I

9.4 CODE MANAGER ASSESSMENT



REC Parties, non-Party Service Users and Service Providers

Overview

An assessment will be conducted by the Code Manager on Parties in order to assess processes / operations are being handled in line with the REC. This may involve on site visits, depending on the nature of the assessment. Where Parties are identified by the Code Manager as failing to meet specific Code obligations by the Code Manager assessment, remediation techniques will be applied. Unlike an annual audit, Parties may be assessed multiple times within the year, or not at all. If a Party is assessed or not will be driven entirely by performance and risk data, so for Parties complying with their obligations under the REC, this technique may be applied infrequently or not at all.

How this will be used

Code Manager assessments will be used to ascertain the extent to which the business is complying with its obligations under the REC. In areas where the organisation is not meeting its obligations the Code Manager will assess the extent of non-compliance and report findings and remediation required (such as an action plan) to both the Party and the PAB. This will enable problematic areas to be addressed and subsequently optimise performance.

Controls in place over its use

1. The scope of the Code Manager assessment is communicated to the Party before the assessment.
2. Information is requested in advance of the commencement of fieldwork.
3. Formal deadlines for Code Manager assessments are approved before use by the PAB.
4. The Code Manager will communicate when this technique is complete, and any specific actions that are required from the assessed organisation.
5. Code Manager notifies the PAB of the outcomes of the assessment.

RACI matrix setting out delegated authority for applying or changing techniques			
	PAB	Code Manager	REC Parties
Changes to the assessment approach taken relating to a specific risk event.	C	R / A	I





10. REMEDIATION TECHNIQUES

Action Plan

Periodic Monitoring and Closure Reports

Management Assertion

Code Manager / Independent Validation

10. REMEDIATION TECHNIQUES



REC Parties, non-Party Service Users and Service Providers

10.1 ACTION PLAN

Overview

The Code Manager can set action plans for REC Parties, Service Users and Service Providers if it assesses that either there is evidence that they are not meeting the obligations, requirements and standards as set out in the REC, or they are likely to not comply unless they take specific action. This may be based on evidence collected through performance assurance data collection, SLA performance data, information that Parties are required to publish, information from a dispute, direct assessment or other sources. The Code Manager may ask the Party to propose an action plan or set specific actions. Parties are expected to submit evidence via the REC Portal to show actions have been completed and progress against action deadlines will be monitored by the Code Manager.

How this will be used

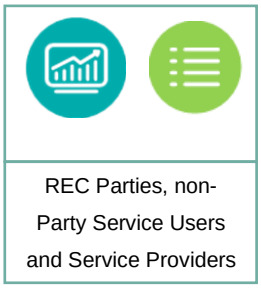
Action plans will be used as a remediation technique to monitor the progress of improvement and evidence there is a plan in place to resolve issues.

Controls in place over its use

1. Action plans are recorded in the REC Portal but will only be visible privately to the Party concerned and the Code Manager. Through access to the REC Portal, Parties be able to provide updates on progress completing actions and request closure.
2. Parties should suggest timescales for action plans and issues being resolved, which the Code Manager will review and challenge (as appropriate) to make sure the timescales are reasonable and proportionate.
3. The Code Manager will assess evidence to confirm that actions have been completed prior to authorising closure. The REC Portal has the functionality to track actions, responses and alert on overdue actions.

RACI matrix setting out delegated authority for applying or changing techniques			
	PAB	Code Manager	REC Parties
Changes to information requested as part of the action plan.	C	R / A	I

10.2 PERIODIC MONITORING AND CLOSURE REPORTS



REC Parties, non-Party Service Users and Service Providers

Overview

Where significant findings have been identified, instead of relying solely on Parties to provide updates, closer monitoring of improvement activity and performance improvement will be required. Periodic monitoring will be performed to check that action plans are being followed and issues are being resolved effectively. Closure reports will evidence that the Code Manager is satisfied that the issue has been resolved and the incident can be closed.

How this will be used

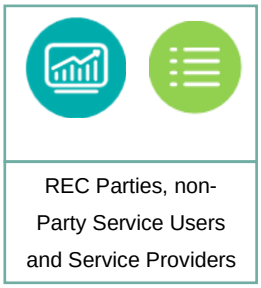
Periodic monitoring will be used by the Code Manager to track progress against action plans and validate that steps are being taken to remediate actions. It will also be used to trigger additional escalation as required.

Controls in place over its use

1. The Code Manager will feed in findings from periodic monitoring to monthly / quarterly updates to the PAB.
2. ~~The REC Portal notifies~~ Parties will be notified via the REC Portal when periodic monitoring is due to take place~~, which will be an automatic notification once an action plan is required~~.
3. The Code Manager can require organisations to provide a closure report and sufficient evidence of action closure for any action plan that is set.
4. Once the Code Manager concludes on a report, it will communicate this to the affected organisation.

RACI matrix setting out delegated authority for applying or changing techniques			
	PAB	Code Manager	REC Parties
Changes to how Parties are notified about periodic monitoring.	I	R / A	I

10.3 MANAGEMENT ASSERTION



REC Parties, non-Party Service Users and Service Providers

Overview

The Code Manager will request a Management Assertion from senior management of REC Parties in response to an identified issue. This will be tailored to the specific circumstances of the issue, but could include acknowledging the issues identified, confirming awareness of their responsibilities, confirmation of actions they will take, or events they will prevent from taking place. This declaration must be approved by an identified member of the Executive team, responsible for compliance, or the Party's Board who have received assurance that they will comply.

How this will be used

Assertions will be used when the Code Manager determines that a Party's performance or circumstances needs them to reconfirm their commitment to market standards. The statement required will be tailored based on the events that triggered the application of this PAT. For example, if an assertion is required following customer detriment caused by a system error, the assertion will be focused on acknowledgment of the issue, the resolution of the system error, rectification of harms caused to customers and prevention of reoccurrence of similar failures.

Controls in place over its use

1. The Code Manager will issue a letter to the Directors of the REC Party or REC Service Provider (as per Companies House) requiring a Management Assertion. This will be issued both via registered post to their registered address (as per Companies House) and the REC Portal.
2. The letter will outline all points the Management Assertion is required to cover.
3. Failure of a REC Party to respond to a Management Assertion will be escalated to PAB.
4. The Code Manager will confirm if it receives a satisfactory management assertion, or specific feedback if it is not satisfactory.

RACI matrix setting out delegated authority for applying or changing techniques			
	PAB	Code Manager	REC Parties
Changes to information required from Management Assertion.	A	R	I

10.4 CODE MANAGER / INDEPENDENT VALIDATION



REC Parties, non-Party Service Users and Service Providers

Overview

Following a serious issue, validation that the issue has been satisfactorily resolved is required. This will be conducted by either the Code Manager or an Independent Provider. This may involve on site visits, depending on the nature of the assessment. This differs from the Code Manager Assessment technique in the nature and extent of procedures. Code Manager Assessments are triggered when performance data indicates issues, which are confirmed or refuted by assessment. This validation technique is used where serious issues have been identified and confirmed, to validate that the identified issue has been fully resolved. It therefore involves more thorough testing, often looking at specific cases.

Depending on the Party type and the nature of the issue, this could involve additional assessments by an independent assessor, such as a metering scheme assessor, or by an independent provider appointed by the Party with suitable skills and experience. In such cases, a copy of the terms of reference and the full final report must be provided to and agreed on with the Code Manager.

How this will be used

Code Manager / Independent Validation will be used as a remediation technique to ascertain the extent to which the business has resolved previously identified issues and bedded in controls to prevent reoccurrence. In areas where the organisation is not meeting the standards set within the Code, the Code Manager will assess the extent of failure, discuss and confirm the factual accuracy with the Party and report to findings and recommend appropriate actions to the PAB. The PAB will then issue further instruction as required. This will enable problematic areas to be addressed and subsequently optimise performance. The appointment of an Independent Assessor and completion of the review, including any requirement for reassessment, will be at a cost to the REC Party or Service Provider.

Controls in place over its use

1. The scope of the Code Manager / Independent Validation is defined and communicated to the Party before the assessment.
2. Information is requested in advance of the commencement of Code Manager validation fieldwork.
3. Formal deadlines for Code Manager / Independent Validation are approved before by the PAB.
4. PAB approval when Code Manager / Independent Validation is required.

RACI matrix setting out delegated authority for applying or changing techniques			
	PAB	Code Manager	REC Parties
Changes to the assessment approach taken relating to a specific risk event.	C	R / A	I





11. ESCALATION TECHNIQUES

Specific Conditions

Referral to Ofgem

Event of Default

11. ESCALATION TECHNIQUES



REC Parties, non-Party Service Users and Service Providers

11.1 SPECIFIC CONDITIONS

Specific conditions will set the parameters for which Parties can operate within the market. They will act as a customer protection to set appropriate limits on Parties who are either new to the market or the Code Manager have identified as being in breach of market standards. It will also be used to cover Controlled Market Entry.

How this will be used

Specific conditions will be used to protect customers and drive performance standards. The Code Manager will assess the appropriateness of specific conditions based on current performance and adherence to market standards. The Code Manager will also use Performance Assurance Techniques to assess whether specific conditions are necessary. For example, if periodic monitoring or sentiment analysis flags an issue with responding to customer complaints, a specific condition could be imposed to set restrictions on operations until the issue has been resolved. The Code Manager would make recommendations to the PAB for the use of this technique, which would require PAB approval to apply.

Controls in place over its use

1. The application of this technique is subject to PAB approval.
2. The criteria for imposing the specific condition will be communicated to the Party along with the evidence requirement for demonstrating significant progress for the removal of the specific condition.
3. Additional specific conditions could be applied, subject to consultation and dependent on PAB approval.
4. The specific conditions will be communicated to the affected organisation.
5. If the specific conditions are removed, this will be communicated to the affected organisation.

RACI matrix setting out delegated authority for applying or changing techniques			
	PAB	Code Manager	REC Parties
Changes to the types of conditions available for use (i.e., a new type of restriction).	R	A	C

11.2 REFERRAL TO OFGEM



REC Parties, non-Party Service Users and Service Providers

Overview

If licensed Parties repeatedly fail to comply with or is in serious breach of regulations and set standards, they could be referred to Ofgem. In such cases, Parties would be identified by the Code Manager, and this would be communicated to the PAB and RECCo. The Code Manager will have the ability to refer to Ofgem at any time if they deem it necessary, subject to PAB or RECCo Board approval.

How this will be used

Referral to Ofgem will predominantly be used only where significant underperformance is identified. In some cases, it may be used prior to qualification being removed. It will be used on occasions where Parties repeatedly fail to comply with market standards and other remediation techniques have been unsuccessful. It could also be used more immediately, in cases where a Party's behaviour or actions are concerning, and consequences of these actions deemed severe.

Controls in place over its use

1. Referrals to Ofgem will require PAB or RECCo Board approval.
2. Both Ofgem and the affected organisations will be notified of this referral.

RACI matrix setting out delegated authority for applying or changing techniques			
	PAB	Code Manager	REC Parties
Decisions on what information to refer about which organisation	R/A	-	I

11.3 EVENT OF DEFAULT



REC Parties, non-Party Service Users and Service Providers

Overview

Market activities are monitored, with Parties failing to comply with regulations and set standards subject to a potential of Event of Default consequences being triggered, as set out in Clause 16 of the REC. This will be identified by the Code Manager, approved by the PAB and communicated to RECCo. The Code Manager, subject to approval from the PAB, will have the ability suspend all of the Party's accounts and restrict access to all REC Services if they deem it necessary.

How this will be used

Triggering an Event of Default and the associated consequences will be used as a form of last resort escalation for Parties who continue to breach the REC in a significant way which impacts customers or other Parties, such as participating in fraudulent activities. It will mean that Parties who do not comply can be suspended from the market and cannot use REC services in the future if they continue to fail to comply.

As this action results in Parties becoming in breach of their licence conditions, the PAB and Code Manager will consult with Ofgem prior to decisions being made about triggering the Event of Default so that Ofgem can take action to protect consumers if required, such as the supplier of last resort provisions.

Controls in place over its use

1. The triggers for an Event of Default are publicly outlined in the REC Main Body, and the specific procedures for its application are outlined in Performance Assurance Schedule and in the PAB Procedures document. ~~Standard thresholds developed to outline the criteria for when an Event of Default can be used, communicated to Parties in advance through high-quality guidance.~~
2. Formal notifications and warnings to Parties once triggers have been reached.
3. The Code Manager will produce evidence case for the Event of Default, ahead of PAB discussion.
4. PAB approval to enact the Event of Default~~,~~; PAB may also elect to consult more widely, e.g. with the Authority, if appropriate.~~ subject to consultation with Ofgem~~.

RACI matrix setting out delegated authority for applying or changing techniques			
	PAB	Code Manager	REC Parties
Recommendations on default to the RECCo Board	A	R	I



To find out more please contact:

performanceassurance@recmanager.co.uk

RETAIL ENERGY CODE